

2013 DRAFTING REQUEST**Assembly Substitute Amendment (ASA-AB218)**

Received: 7/17/2013

Received By: gmalaise

Wanted: 7/19/2013 4:00:00 PM

Same as LRB:

For: Melissa Sargent (608) 266-0960

By/Representing: Aaron Collins

May Contact:

Drafter: gmalaise

Subject: Employ Priv - miscellaneous
Privacy

Addl. Drafters:

Extra Copies:

Submit via email: YES

Requester's email: Rep.Sargent@legis.wisconsin.gov

Carbon copy (CC) to:

Pre Topic:

No specific pre topic given

Topic:

Employer, educational institution, and landlord access to employee, student, and tenant personal Internet accounts

Instructions:

See attached--draft up agreed-to compromise attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	gmalaise 7/17/2013	jdyer 7/18/2013	rschluet 7/18/2013	_____			
/1	gmalaise 8/7/2013			_____	mbarman 7/18/2013	mbarman 7/18/2013	
/2		scalvin 8/13/2013	rschluet 8/14/2013	_____	sbasford 8/14/2013	sbasford 8/14/2013	

FE Sent For:

<END>

2013 DRAFTING REQUEST

Assembly Substitute Amendment (ASA-AB218)

Received: 7/17/2013 Received By: gmalaise
Wanted: 7/19/2013 4:00:00 PM Same as LRB:
For: Melissa Sargent (608) 266-0960 By/Representing: Aaron Collins
May Contact: Drafter: gmalaise
Subject: Employ Priv - miscellaneous Addl. Drafters:
Privacy Extra Copies:

Submit via email: YES
Requester's email: Rep.Sargent@legis.wisconsin.gov
Carbon copy (CC) to:

Pre Topic:

No specific pre topic given


Topic:

Employer, educational institution, and landlord access to employee, student, and tenant personal Internet accounts

Instructions:

See attached--draft up agreed-to compromise attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	gmalaise 7/17/2013	jdye 7/18/2013	rschluet 7/18/2013	_____			
/1				_____	mbarman 7/18/2013	mbarman 7/18/2013	
FE Sent For:		12 sac 08/13/2013					

<END>

2013 DRAFTING REQUEST

Assembly Substitute Amendment (ASA-AB218)

Received: 7/17/2013 Received By: gmalaise
 Wanted: 7/19/2013 4:00:00 PM Same as LRB:
 For: Melissa Sargent (608) 266-0960 By/Representing: Aaron Collins
 May Contact: Drafter: gmalaise
 Subject: Employ Priv - miscellaneous Addl. Drafters:
 Privacy Extra Copies:

Submit via email: YES
 Requester's email: Rep.Sargent@legis.wisconsin.gov
 Carbon copy (CC) to:

Pre Topic:

No specific pre topic given

Topic:

Employer, educational institution, and landlord access to employee, student, and tenant personal Internet accounts

Instructions:

See attached--draft up agreed-to compromise attached

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	gmalaise	7/18 jld	7/18/13				

FE Sent For:

<END>

2013 ASSEMBLY BILL 218

May 24, 2013 - Introduced by Representatives SARGENT, BIES, BARCA, BARNES, BERCEAU, BERNARD SCHABER, BEWLEY, BILLINGS, CLARK, DANOU, DOYLE, GENRICH, GOYKE, HEBL, HESSELBEIN, HINTZ, HULSEY, JOHNSON, JORGENSEN, KAHL, KESSLER, KOLSTE, MASON, MILROY, OHNSTAD, A. OTT, PASCH, POPE, RICHARDS, RIEMER, RINGHAND, SINICKI, SMITH, C. TAYLOR, VRUWINK, WACHS, WRIGHT, YOUNG, ZAMARRIPA, ZEPNICK^{swe}, BERNIER and JAGLER, cosponsored by Senators GROTHMAN, LEHMAN, LASEE, ERPENBACH, HANSEN, HARRIS, C. LARSON, MILLER, RISSER and L. TAYLOR. Referred to Committee on Government Operations and State Licensing.

1 AN ACT *to amend* 111.322 (2m) (a) and 111.322 (2m) (b); and *to create* 106.54 (10),
2 111.91 (2) (im) and 995.55 of the statutes; **relating to:** employer access to, and
3 observation of, the personal Internet accounts of employees and applicants for
4 employment; educational institution access to, and observation of, the personal
5 Internet accounts of students and prospective students; landlord access to, and
6 observation of, the personal Internet accounts of tenants and prospective tenants;
7 and providing a penalty.

Analysis by the Legislative Reference Bureau

Current law does not regulate employer access to, or observation of, the personal Internet accounts of employees and applicants for employment, or educational institution access to, or observation of, the personal Internet accounts of students and prospective students, or landlord access to, or observation of, the personal Internet accounts of tenants and prospective tenants.

This bill prohibits an employer, educational institution, or landlord from: 1) requesting an employee, applicant for employment, student, prospective student, tenant, or prospective tenant to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the employee, applicant, student, prospective student, tenant, or prospective tenant; and 2) discharging, expelling, suspending, disciplining, or otherwise penalizing or discriminating against any person for exercising the right to refuse such a request, opposing such a practice, filing a complaint or attempting to enforce that right, or testifying or assisting in any action or proceeding to enforce that right.

The bill, however, permits an employer, educational institution, or landlord to view, access, or use information about an employee, applicant for employment, student, prospective student, tenant, or prospective tenant that can be obtained without access information or that is available from the public domain.

The bill also permits an employer or educational institution to request or require an employee or student to disclose access information to the employer or educational institution in order for the employer or educational institution to gain access to or operate an electronic communications device paid for in whole or in part by the employer or educational institution or to gain access to an account or service that is provided by the employer or educational institution, that the employee or student obtained by virtue of the employment relationship or admission to the educational institution, or that is used for business or educational purposes.

The bill, in addition, permits an employer to do any of the following:

1. Discharge or discipline an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.
2. Conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account or of any other alleged employment-related misconduct or violation of the law.
3. Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device paid for in whole or in part by the employer or while using the employer's network or other resources.
4. Monitor, review, or access electronic data that is stored on an electronic communications device paid for in whole or in part by the employer or electronic data that is traveling through or stored on the employer's network.
5. Comply with a duty to screen applicants for employment prior to hiring that is established under state or federal law or by a self-regulatory organization, as defined under the federal Securities and Exchange Act of 1934 (self-regulatory organization).
6. Requesting or requiring an employee to disclose the employee's personal electronic mail address.

In addition, with respect to an employer, the bill provides that the prohibition created under the bill does not apply to a personal Internet account or an electronic communications device of an employee engaged in providing financial services who uses the account or device to conduct the business of an employer that is subject to the content, supervision, and retention requirements imposed by federal securities laws and regulations or by a self-regulatory organization.

Finally, the bill provides that an employer, educational institution, or landlord does not have a duty to search or monitor the activity of any personal Internet account and that an employer, educational institution, or landlord is not liable for any failure to request or require access to or observation of a personal Internet account of an employee, applicant for employment, student, prospective student, tenant, or prospective tenant.

For purposes of the bill: 1) "access information" means a user name and password, login information, or any other security information that protects access to a personal Internet account; 2) "educational institution" means an institution of higher education, a technical college, a proprietary school, a public school, a charter school, a private school, or a private educational testing service or administrator; 3) "employer" includes the state; and 4) "personal Internet

account” means an account created and used exclusively for personal purposes within a bounded system established by an Internet-based service that requires a user to input or store access information via an electronic device in order to view, create, use, or edit the user’s account information, profile, display, communications, or stored data.

For further information see the *state and local* fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

1 **SECTION 1.** 106.54 (10) of the statutes is created to read:

2 106.54 (10) (a) The division shall receive complaints under s. 995.55 (6)

3 (b) and shall process the complaints in the same manner as employment
4 discrimination complaints are processed under s. 111.39.

5 (b) The division shall receive complaints under s. 995.55 (6) (c) and shall
6 process the complaints in the same manner as housing discrimination complaints
7 are processed under s. 106.50.

8 **SECTION 2.** 111.322 (2m) (a) of the statutes is amended to read:

9 111.322 (2m) (a) The individual files a complaint or attempts to enforce
10 any right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455,
11 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, 995.55.~~ or ss.
12 101.58 to 101.599 or 103.64 to 103.82.

13 **SECTION 3.** 111.322 (2m) (b) of the statutes is amended to read:

14 111.322 (2m) (b) The individual testifies or assists in any action or
15 proceeding held under or to enforce any right under s. 103.02, 103.10, 103.13,
16 103.28, 103.32, 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07,
17 109.075, ~~or 146.997, 995.55,~~ or ss. 101.58 to 101.599 or 103.64 to 103.82.

18 **SECTION 4.** 111.91 (2) (im) of the statutes is created to read:

1 111.91 (2) (im) Employer access to the social networking Internet site of
2 an employee that provides fewer rights and remedies to employees than are
3 provided under s. 995.55.

4 SECTION 5. 995.55 of the statutes is created to read:

5 995.55 Internet privacy protection. (1) DEFINITIONS. In this section:

6 (a) "Access information" means a user name and password, login
7 information,¹ or any other security information that protects access to a personal
8 Internet account.

9 (b) "Educational institution" means an institution of higher education,
10 as defined in s. 108.02 (18); a technical college established under s. 38.02; a
11 school, as defined in s. 38.50 (11) (a) 2.; a public school, as described in s. 115.01
12 (1); a charter school, as defined in s. 115.001 (1); a private school, as defined in
13 s. 115.001 (3r); or a private educational testing service or administrator.

14 (c) "Employer" means any person engaging in any activity, enterprise,
15 or business employing at least one individual. "Employer" includes the state, its
16 political subdivisions, and any office, department, independent agency, authority,
17 institution, association, society, or other body in state or local government created
18 or authorized to be created by the constitution or any law, including the legislature
19 and the courts.

20 (d) "Personal Internet account" means an account created and used
21 exclusively for personal purposes ~~within a bounded system established by an~~
22 ~~Internet-based service that requires a user to input or store access information via~~

¹ The term "login information" is undefined, confusing and unnecessary, as "user name and password" and "other security information" are already specified here.

No
Circular
w/encs
del.

1 ~~an electronic device in order to view, create, use, or edit the user's account~~
2 ~~information, profile, display, communications, or stored data.~~²

3 (2) RESTRICTIONS ON EMPLOYER ACCESS TO PERSONAL
4 INTERNET ACCOUNTS, (a) Except as provided in pars, (b) and (c), no
5 employer may do any of the following:

6 1. Request ~~or require~~³ ~~an employee or applicant for employment to~~
7 ~~grant access to, allow observation of, or disclose~~ ~~access~~ ~~information~~ ~~for that allows~~
8 ~~access to or observation of~~ the personal Internet account of the employee or
9 applicant.

10 2. Discharge, ~~discipline~~ or otherwise discriminate against ~~penalize or~~
11 ~~threaten to discharge, discipline or otherwise penalize an employee solely for not~~
12 ~~disclosing access information~~ any person for exercising the right to refuse a
13 request under subd. 1., opposing a practice prohibited under subd. 1., filing a
14 complaint or attempting to enforce any right under subd. 1., or testifying or
15 assisting in any action or proceeding to enforce any right under subd. 1.

16 3. ~~Fail or refuse to hire any applicant for employment as a result of the~~
17 ~~applicant's refusal to disclose access information.~~⁴ ~~OK~~

18 (b) Paragraph (a) does not prohibit an employer from doing any of the
19 following:

20 1. Requesting or requiring an employee to disclose access
21 information to the employer in order for the employer to gain access to or operate

² This change provides a clear definition of the term "personal Internet account," similar to ones used in other states.

³ This change makes the bill internally consistent and consistent with social media privacy bills in other states, which prohibit employers from requesting or requiring an employee or applicant to disclose access information that allows access to an employee's or applicant's personal Internet account.

⁴ These clarifying changes to the bill's prohibitions strengthen the bill and make it more consistent with social media privacy bills in other states.

OK
1 an electronic communications device supplied⁵ or paid for in whole or in part by
2 the employer or to gain access to an account or service that is provided by the
3 employer, that the employee obtained by virtue of the employee's employment
4 relationship with the employer, or that is used for the employer's business
5 purposes.

6 2. Discharging or disciplining an employee for transferring the
7 employer's proprietary or confidential information or financial data to the
8 employee's personal Internet account without the employer's authorization.

9 3. Conducting an investigation or requiring an employee to cooperate
10 in an investigation of any alleged unauthorized transfer of the employer's
11 proprietary or confidential information or financial data to the employee's
12 personal Internet account, if the employer has reasonable cause to believe that
13 such a transfer has occurred, or of any other alleged employment-related
14 misconduct or violation of the law, if the employer has reasonable cause to
15 believe that activity on the employee's personal Internet account relating to that
16 misconduct or violation of the law has occurred. Conducting an investigation or
17 requiring an employee to cooperate in an investigation as specified in this
18 subsection includes requiring the employee to share ~~the~~ content that has been
19 reported ^{to the employer} ^{about the matter being investigated} in order to make a factual determination, without obtaining the user
20 name and password to the employee's personal Internet account.⁶ OK

*
⁵ This change would cover any electronic communications devices supplied by the employer (in addition to subsidized device programs, as originally included in the bill).

⁶ This language clarifies that the employer can review the specific content of the account, but does NOT say that the employer can actually obtain the user name and password. This would remain prohibited.

Footnote is actually clearer

1 4. Restricting or prohibiting an employee's access to certain Internet
2 sites while using an electronic communications device paid for in whole or in part
3 by the employer or while using the employer's network or other resources.

4 5. If through the use of an electronic device or program that monitors
5 an employer's network or the use of employer provided devices, an employer
6 inadvertently receives an employee's username and password, password, or other
7 access information, the employer is not liable for having this information, but may
8 not use this information to access an employee's personal online
9 account. ~~Monitoring, reviewing, or accessing electronic data that is stored on an~~
10 ~~electronic communications device paid for in whole or in part by the employer or~~
11 ~~electronic data that is traveling through or stored on the employer's network.~~⁷

key
of - life issues

12 6. Complying with a duty to screen applicants for employment prior
13 to hiring or to monitor or retain employee communications⁸ ~~that is established~~
14 ~~underin accordance with~~ state or federal law or rules of ~~by~~ a self-regulatory
15 organization, as defined in 15 USC 78c (a) (26).

16 7. Viewing, accessing, or using information about an employee or
17 applicant for employment that can be obtained without access information or that
18 is available in the public domain.

19 8. Requesting or requiring an employee to disclose the employee's
20 personal electronic mail address.

21 (c) Paragraph (a) does not apply to a personal Internet account or an
22 electronic communications device of an employee engaged in providing financial

⁷ This is a narrower version of the employer monitoring exception that our coalition agreed to with the national ACLU and that has been enacted in other states, such as Washington and Oregon.

⁸ Certain employers, such as those in the financial services industry, have legal obligations under various laws and rules/regulations of self-regulatory organizations to check employees' personal Internet accounts. This clarifies that such employers are permitted to comply with these mandates.

1 services who uses the account or device to conduct the business of an employer
2 that is subject to the content, supervision, and retention requirements imposed by
3 federal securities laws and regulations or by a self-regulatory organization, as
4 defined in 15 USC 78c (a) (26).

5 (3) RESTRICTIONS ON EDUCATIONAL INSTITUTION ACCESS
6 TO PERSONAL INTERNET ACCOUNTS, (a) Except as provided in par. (b), no
7 educational institution may do any of the following:

8 1. Request a student or prospective student to grant access to, allow
9 observation of, or disclose information that allows access to or observation of the
10 personal Internet account of the student or prospective student.

11 2. Expel, suspend, discipline, or otherwise penalize any student or
12 prospective student for exercising the right to refuse a request under subd. 1.,
13 opposing a practice prohibited under subd. 1., filing a complaint or attempting to
14 enforce any right under subd. 1., or testifying or assisting in any action or
15 proceeding to enforce any right under subd. 1.

16 (b) Paragraph (a) does not prohibit an educational institution from doing
17 any of the following:

18 1. Requesting or requiring a student to disclose access information to
19 the educational institution in order for the institution to gain access to or operate
20 an electronic communications device paid for in whole or in part by the institution
21 or to gain access to an account or service that is provided by the institution, that
22 the student obtained by virtue of the student's admission to the educational
23 institution, or that is used by the student for educational purposes.

UOSL

1 2. Viewing, accessing, or using information about a student or
2 prospective student that can be obtained without access information or that is
3 available in the public domain.

4 **(4) RESTRICTIONS ON LANDLORD ACCESS TO PERSONAL**
5 **INTERNET ACCOUNTS, (a)**

6 Except as provided in par. (b), no landlord may do any of the following:

7 1. Request a tenant or prospective tenant to grant access to, allow
8 observation of, or disclose information that allows access to or observation of the
9 personal Internet account of the tenant or prospective tenant.

10 2. Discriminate in a manner described in s. 106.50 (2) against a
11 tenant or prospective tenant for exercising the right to refuse a request under subd.
12 1., opposing a practice prohibited under subd. 1., filing a complaint or attempting
13 to enforce any right under subd. 1., or testifying or assisting in any action or
14 proceeding to enforce any right under subd. 1.

15 (b) Paragraph (a) does not prohibit a landlord from viewing, accessing, or
16 using information about a tenant or prospective tenant that can be obtained
17 without access information or that is available in the public domain.

18 **(5) No DUTY TO MONITOR.** (a) Nothing in this section creates a
19 duty for an employer, educational institution, or landlord to search or monitor the
20 activity of any personal Internet account.

21 (b) An employer, educational institution, or landlord is not liable under
22 this section for any failure to request or require that an employee, applicant for
23 employment, student, prospective student, tenant, or prospective tenant grant
24 access to, allow observation of, or disclose information that allows access to or

1 2. Viewing, accessing, or using information about a student or
2 prospective student that can be obtained without access information or that is
3 available in the public domain.

4 **(4) RESTRICTIONS ON LANDLORD ACCESS TO PERSONAL**
5 **INTERNET ACCOUNTS, (a)**

6 Except as provided in par. (b), no landlord may do any of the following:

7 1. Request a tenant or prospective tenant to grant access to, allow
8 observation of, or disclose information that allows access to or observation of the
9 personal Internet account of the tenant or prospective tenant.

10 2. Discriminate in a manner described in s. 106.50 (2) against a
11 tenant or prospective tenant for exercising the right to refuse a request under subd.
12 1., opposing a practice prohibited under subd. 1., filing a complaint or attempting
13 to enforce any right under subd. 1., or testifying or assisting in any action or
14 proceeding to enforce any right under subd. 1.

15 (b) Paragraph (a) does not prohibit a landlord from viewing, accessing, or
16 using information about a tenant or prospective tenant that can be obtained
17 without access information or that is available in the public domain.

18 **(5) No DUTY TO MONITOR.** (a) Nothing in this section creates a
19 duty for an employer, educational institution, or landlord to search or monitor the
20 activity of any personal Internet account.

21 (b) An employer, educational institution, or landlord is not liable under
22 this section for any failure to request or require that an employee, applicant for
23 employment, student, prospective student, tenant, or prospective tenant grant
24 access to, allow observation of, or disclose information that allows access to or

1 observation of a personal Internet account of the employee, applicant for
2 employment, student, prospective student, tenant, or prospective tenant.

3 (6) ENFORCEMENT. (a) Any person who violates sub. (2) (a), (3)
4 (a), or (4) (a) may be required to forfeit not more than \$1,000.

5 (b) An employee or applicant for employment who is discharged or
6 otherwise discriminated against in violation of sub. (2) (a) 2. or a student or
7 prospective student who is expelled, suspended, disciplined, or otherwise
8 penalized in violation of sub. (3) (a) 2. may file a complaint with the department,
9 and the department shall process the complaint in the same manner as
10 employment discrimination complaints are processed under s. 111.39. If the
11 department finds that a violation of sub. (2) (a) 2. or (3) (a) 2. has been
12 committed, the department may order the employer or educational institution to
13 take such action authorized under s. 111.39 as will remedy the violation. Section
14 111.322 (2m) applies to a discharge or other discriminatory act arising in
15 connection with any proceeding under this paragraph.

16 (c) A tenant or prospective tenant who is discriminated against in violation
17 of sub. (4) (a) 2. may file a complaint with the department, and the department
18 shall process the complaint in the same manner as housing discrimination
19 complaints are processed under s. 106.50. If the department finds that a violation
20 of sub. (4) (a) 2. has been committed, the department may order the landlord to
21 take such action authorized under s. 106.50 as will remedy the violation.

22 **SECTION 6. Initial applicability.**

23 (1) COLLECTIVE BARGAINING AGREEMENT. This act first applies
24 to an employee who is affected by a collective bargaining agreement that contains

1 provisions inconsistent with this act on the day on which the collective bargaining
2 agreement expires or is extended, modified, or renewed, whichever occurs first.

3 (END)

Malaise, Gordon

From: Malaise, Gordon
Sent: Wednesday, July 17, 2013 11:56 AM
To: Collins, Aaron
Subject: RE: AB 218 sub

Aaron:

I have it drafted, but will key it in today, which will make life easier for our editors and typists and result in the draft getting out sooner.

When you receive the draft, you will see that it varies a little bit from what we discussed in the following areas:

1. Definition of "personal Internet account." In researching a little bit what other states are doing, I found that LA's original bill had the long, involved definition, but that their substitute amendment has a shorter, more straightforward definition. So I drafted up the LA definition, which is similar to the submitted definition, but has more content to it in that it clarifies that it is an *Internet-based* account created and used *by an individual exclusively for purposes of personal communications*.
2. Restrictions on employer access. The substitute amendment will retain the prohibitions on granting access and allowing observation because an employer could sidestep the intent of the law by not requiring disclosure of access information, but requiring the employee to grant access or allow observation and then looking over the employee's shoulder at the employee's account. I think we need to keep references to granting access and allowing observation to keep this provision consistent with the exception for conducting an investigation. See item 4. Below.
3. Employer monitoring. I had suggested keeping the language from the bill, but adding the compromise language. On further review, even though as a drafter I think I can do it better, the stakeholders did agree to a compromise, so I went ahead and drafted up their compromise. Returning to the LA language, LA's original bill resembled our original bill with respect to monitoring, but their substitute amendment resembles the compromise language submitted to you.
4. Conducting an investigation. Footnote No. 6 of the submitted language is actually clearer and more straightforward than the draft language, so I drafted up the footnote instead of the draft language, i.e., in conducting an investigation the employer can require an employee to grant access to or allow observation of the account, but cannot require disclosure of access information for the account.

By the way, I e-mailed your dad and told him that I met a smart, pleasant young man from Rep. Sargent's office. He thanked me for my kind words all the way from Bath, England. I think I made his day. ☺

Gordon

From: Collins, Aaron
Sent: Wednesday, July 17, 2013 11:22 AM
To: Malaise, Gordon
Subject: AB 218 sub

Hi Gordon,

Just wanted to touch base to see if you'd had a chance to get the substitute amendment drafted for the social media bill. Thanks!

Aaron Collins

Office of Representative Melissa Sargent

48th Assembly District

8 West, State Capitol

608-266-0960

aaron.collins@legis.wi.gov



State of Wisconsin
2013 - 2014 LEGISLATURE



LRB-1651/3

GMM:eev:jm

ASSEMBLY SUBSTITUTE AMENDMENT
TO

2013 ASSEMBLY BILL 218

May 24, 2013 - Introduced by Representatives SARGENT, BIES, BARCA, BARNES, BERCEAU, BERNARD SCHABER, BEWLEY, BILLINGS, CLARK, DANOU, DOYLE, GENRICH, GOYKE, HEBL, HESSELBEIN, HINTZ, HULSEY, JOHNSON, JORGENSEN, KAHL, KESSLER, KOLSTE, MASON, MILROY, OHNSTAD, A. OTT, PASCH, POPE, RICHARDS, RIEMER, RINGHAND, SINICKI, SMITH, C. TAYLOR, VRUWINK, WACHS, WRIGHT, YOUNG, ZAMARRIPA, ZEPNICK, BERNIER and JACLER, cosponsored by Senators GROTHMAN, LEHMAN, LASEE, ERPENBACH, HANSEN, HARRIS, C. LARSON, MILLER, RISSE and L. TAYLOR. Referred to Committee on Government Operations and State Licensing.

- 1 AN ACT *to amend* 111.322 (2m) (a) and 111.322 (2m) (b); and *to create* 106.54
2 (10), 111.91 (2) (im) and 995.55 of the statutes; **relating to:** employer access to,
3 and observation of, the personal Internet accounts of employees and applicants
4 for employment; educational institution access to, and observation of, the
5 personal Internet accounts of students and prospective students; landlord
6 access to, and observation of, the personal Internet accounts of tenants and
7 prospective tenants; and providing a penalty.

substitute amendment

Analysis by the Legislative Reference Bureau

Current law does not regulate employer access to, or observation of, the personal Internet accounts of employees and applicants for employment, or educational institution access to, or observation of, the personal Internet accounts of students and prospective students, or landlord access to, or observation of, the personal Internet accounts of tenants and prospective tenants.

or requiring

This ~~bill~~ prohibits an employer, educational institution, or landlord from: 1) requesting an employee, applicant for employment, student, prospective student, tenant, or prospective tenant to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the employee, applicant, student, prospective student, tenant, or prospective tenant; ~~and~~ 2) discharging, expelling, suspending, disciplining, or otherwise penalizing or

a user name and password or any other security information (access information) that protects access to an Internet-based account that is created and used exclusively for purposes of personal communications (personal Internet account)

to grant that access, allow that observation, or disclose that access information

2013 - 2014 Legislature

- 2 -

LRB-1551/3
GMM:eev:jm

ASSEMBLY BILL 218

on employee, student, tenant, or prospective tenant
discriminating against any person for exercising the right to refuse such a request, opposing such a practice, filing a complaint or attempting to enforce that right, or testifying or assisting in any action or proceeding to enforce that right.

The bill, however, permits an employer, educational institution, or landlord to view, access, or use information about an employee, applicant for employment, student, prospective student, tenant, or prospective tenant that can be obtained without access information or that is available from the public domain.

The bill also permits an employer or educational institution to request or require an employee or student to disclose access information to the employer or educational institution in order for the employer or educational institution to gain access to or operate an electronic communications device paid for in whole or in part by the employer or educational institution, or to gain access to an account or service that is provided by the employer or educational institution, that the employee or student obtained by virtue of the employment relationship or admission to the educational institution, or that is used for business or educational purposes.

The bill, in addition, permits an employer to do any of the following:

1. Discharge or discipline an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.

2. Conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account or of any other alleged employment-related misconduct or violation of the law.

3. Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device paid for in whole or in part by the employer or while using the employer's network or other resources.

4. Monitor, review, or access electronic data that is stored on an electronic communications device paid for in whole or in part by the employer or electronic data that is traveling through or stored on the employer's network.

5. Comply with a duty to screen applicants for employment prior to hiring that is established under state or federal law or by a self-regulatory organization, as defined under the federal Securities and Exchange Act of 1934 (self-regulatory organization).

6. Requesting or requiring an employee to disclose the employee's personal electronic mail address.

In addition, with respect to an employer, the bill provides that the prohibition created under the bill does not apply to a personal Internet account or an electronic communications device of an employee engaged in providing financial services who uses the account or device to conduct the business of an employer that is subject to the content, supervision, and retention requirements imposed by federal securities laws and regulations or by a self-regulatory organization.

Finally, the bill provides that an employer, educational institution, or landlord does not have a duty to search or monitor the activity of any personal Internet account and that an employer, educational institution, or landlord is not liable for

and 2) that an employer that inadvertently obtains access information for an employee's personal Internet account through the use of an electronic device or program that monitors the employer's network or through an employer-provided electronic communications device is not liable under the bill for possessing that access information so long as the employer does not use that access information to access the employee's personal Internet account

ASSEMBLY BILL 218

the purpose of personal
communications

Internet-based

any failure to request or require access to or observation of a personal Internet account of an employee, applicant for employment, student, prospective student, tenant, or prospective tenant.

For purposes of the bill: 1) "access information" means a user name and password, login information, or any other security information that protects access to a personal Internet account; 2) "educational institution" means an institution of higher education, a technical college, a proprietary school, a public school, a charter school, a private school, or a private educational testing service or administrator; 3) "employer" includes the state; and 4) "personal Internet account" means an account created and used exclusively for personal purposes within a bounded system established by an Internet-based service that requires a user to input or store access information via an electronic device in order to view, create, use, or edit the user's account information, profile, display, communications, or stored data.

For further information see the *state and local* fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

1 **SECTION 1.** 106.54 (10) of the statutes is created to read:

2 106.54 (10) (a) The division shall receive complaints under s. 995.55 (6) (b) and
3 shall process the complaints in the same manner as employment discrimination
4 complaints are processed under s. 111.39.

5 (b) The division shall receive complaints under s. 995.55 (6) (c) and shall
6 process the complaints in the same manner as housing discrimination complaints
7 are processed under s. 106.50.

8 **SECTION 2.** 111.322 (2m) (a) of the statutes is amended to read:

9 111.322 (2m) (a) The individual files a complaint or attempts to enforce any
10 right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50,
11 104.12, 106.04, 109.03, 109.07, 109.075, or 146.997, 995.55, or ss. 101.58 to 101.599
12 or 103.64 to 103.82.

13 **SECTION 3.** 111.322 (2m) (b) of the statutes is amended to read:

ASSEMBLY BILL 218

SECTION 3

111.322 (2m) (b) The individual testifies or assists in any action or proceeding held under or to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, 995.55~~, or ss. 101.58 to 101.599 or 103.64 to 103.82.

SECTION 4. 111.91 (2) (im) of the statutes is created to read:

111.91 (2) (im) Employer access to the social networking Internet site of an employee that provides fewer rights and remedies to employees than are provided under s. 995.55.

SECTION 5. 995.55 of the statutes is created to read:

995.55 Internet privacy protection. (1) DEFINITIONS. In this section:

(a) "Access information" means a user name and password, ~~login information~~, or any other security information that protects access to a personal Internet account.

(b) "Educational institution" means an institution of higher education, as defined in s. 108.02 (18); a technical college established under s. 38.02; a school, as defined in s. 38.50 (11) (a) 2.; a public school, as described in s. 115.01 (1); a charter school, as defined in s. 115.001 (1); a private school, as defined in s. 115.001 (3r); or a private educational testing service or administrator.

(c) "Employer" means any person engaging in any activity, enterprise, or business employing at least one individual. "Employer" includes the state, its political subdivisions, and any office, department, independent agency, authority, institution, association, society, or other body in state or local government created or authorized to be created by the constitution or any law, including the legislature and the courts.

(d) "Personal Internet account" means an Internet-based account that is by an individual created and used exclusively ~~for personal purposes within a bounded system established by an Internet-based~~

for the purposes of personal communications

service that requires a user to input or store access information via an electronic device in order to view, create, use, or edit the user's account information, profile, display, communications, or stored data. or require information for a

(2) RESTRICTIONS ON EMPLOYER ACCESS TO PERSONAL INTERNET ACCOUNTS. (a)

Except as provided in pars. (b) and (c), no employer may do any of the following: skt

1. Request an employee or applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the employee or applicant. an employee

2. Discharge or otherwise discriminate against any person for exercising the right to refuse a request under subd. 1., opposing a practice prohibited under subd. 1., filing a complaint or attempting to enforce any right under subd. 1., or testifying or assisting in any action or proceeding to enforce any right under subd. 1. (to refuse to disclose access information for the employee's personal Internet account)

(b) Paragraph (a) does not prohibit an employer from doing any of the following:

1. Requesting or requiring an employee to disclose access information to the employer in order for the employer to gain access to or operate an electronic communications device paid for in whole or in part by the employer or to gain access to an account or service that is provided by the employer, that the employee obtained by virtue of the employee's employment relationship with the employer, or that is used for the employer's business purposes. (supplier or in order for the employee)

2. Discharging or disciplining an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.

3. Conducting an investigation or requiring an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet (Subject to this subdivision, conducting)

3. Refuse to hire an applicant for employment because the applicant refused to grant access to, allow observation of, or disclose access information for the applicant's personal Internet account.

In conducting an investigation or requiring an employee to cooperate in an investigation under this subdivision, an employer may require an employee to grant access to or allow observation of the employee's personal Internet account, but may not require the employee to disclose

2013 - 2014 Legislature

- 6 -

LRB-1551/3

GMM:eev:jm

ASSEMBLY BILL 218

SECTION 5

1 account, if the employer has reasonable cause to believe that such a transfer has
2 occurred, or of any other alleged employment-related misconduct or violation of the
3 law, if the employer has reasonable cause to believe that activity on the employee's
4 personal Internet account relating to that misconduct or violation of the law has
5 occurred.

access
information
for that
account.

or a duty to monitor or retain employee
communications

6 4. Restricting or prohibiting an employee's access to certain Internet sites while
7 using an electronic communications device ^{supplied or} paid for in whole or in part by the
8 employer or while using the employer's network or other resources.

9 ~~5. Monitoring, reviewing, or accessing electronic data that is stored on an~~
10 ~~electronic communications device paid for in whole or in part by the employer or~~
11 ~~electronic data that is traveling through or stored on the employer's network.~~

12 ~~6.~~ 6. Complying with a duty to screen applicants for employment prior to hiring
13 that is established under state or federal law ^{the rules of} or by a self-regulatory organization,
14 as defined in 15 USC 78c (a) (26). ^{laws, rules, or regulations or the rules of}

15 ~~6.~~ 7. Viewing, accessing, or using information about an employee or applicant for
16 employment that can be obtained without access information or that is available in
17 the public domain.

18 ~~7.~~ 8. Requesting or requiring an employee to disclose the employee's personal
19 electronic mail address.

20 (c) Paragraph (a) does not apply to a personal Internet account or an electronic
21 communications device of an employee engaged in providing financial services who
22 uses the account or device to conduct the business of an employer that is subject to
23 the content, supervision, and retention requirements imposed by federal securities
24 laws and regulations or by ^{the rules of a} a self-regulatory organization, as defined in 15 USC 78c

25 (a) (26).

~~Employer does not use that access information to access the employee's
personal Internet account.~~

→ (d) An employer that inadvertently obtains access information for an
employee's personal Internet account through the use of an electronic device that or program
that monitors the employer's network or the use of an employer-provided through an
electronic communication device supplied or paid for in whole or part by the employer, is
not liable under par. (a) for possessing that access information so long as the

(3) RESTRICTIONS ON EDUCATIONAL INSTITUTION ACCESS TO PERSONAL INTERNET ACCOUNTS. (a) Except as provided in par. (b), no educational institution may do any of the following: ^{or require}

1. Request ^{information for a} a student or prospective student to grant access to, allow observation of, or disclose ~~information that allows access to or observation of the~~ personal Internet account of the student or prospective student.

2. Expel, suspend, discipline, or otherwise penalize any student ~~or prospective student~~ for exercising the right to ~~refuse a request~~ under subd. 1), opposing a practice prohibited under subd. 1., filing a complaint or attempting to enforce any right under subd. 1., or testifying or assisting in any action or proceeding to enforce any right under subd. 1.

(b) Paragraph (a) does not prohibit an educational institution from doing any of the following:

1. Requesting or requiring ^{supplied or} a student to disclose access information to the educational institution in order for the institution to gain access to or operate an electronic communications device ^{in order for the institution} paid for in whole or in part by the institution or to gain access to an account or service ~~that is~~ provided by the institution, ~~that the student~~ obtained by virtue of the student's admission to the educational institution, or ~~that is used by the student~~ for educational purposes.

2. Viewing, accessing, or using information about a student or prospective student that can be obtained without access information or that is available in the public domain.

(4) RESTRICTIONS ON LANDLORD ACCESS TO PERSONAL INTERNET ACCOUNTS. (a) Except as provided in par. (b), no landlord may do any of the following:

3. Refuse to admit a prospective student because the prospective student refused to grant access to, allow observation of, or disclose access information for the prospective student's personal Internet account.

ASSEMBLY BILL 218

LBB-1551/3

GMM:eevjm

SECTION 5

1 Request a tenant or prospective tenant to grant access to, allow observation
2 of, or disclose ~~information that allows access to or observation of the~~ personal
3 Internet account of the tenant or prospective tenant.

4 2. Discriminate in a manner described in s. 106.50 (2) against a tenant or
5 prospective tenant for exercising the right to ~~refuse a request~~ under subd. 1,
6 opposing a practice prohibited under subd. 1., filing a complaint or attempting to
7 enforce any right under subd. 1., or testifying or assisting in any action or proceeding
8 to enforce any right under subd. 1.

9 (b) Paragraph (a) does not prohibit a landlord from viewing, accessing, or using
10 information about a tenant or prospective tenant that can be obtained without access
11 information or that is available in the public domain.

12 (5) NO DUTY TO MONITOR. (a) Nothing in this section creates a duty for an
13 employer, educational institution, or landlord to search or monitor the activity of any
14 personal Internet account.

15 (b) An employer, educational institution, or landlord is not liable under this
16 section for any failure to request or require that an employee, applicant for
17 employment, student, prospective student, tenant, or prospective tenant grant
18 access to, allow observation of, or disclose information that allows access to or
19 observation of a personal Internet account of the employee, applicant for
20 employment, student, prospective student, tenant, or prospective tenant.

21 (6) ENFORCEMENT. (a) Any person who violates sub. (2) (a), (3) (a), or (4) (a) may
22 be required to forfeit not more than \$1,000.

23 (b) An employee ~~or applicant for employment~~ who is discharged or otherwise
24 discriminated against in violation of sub. (2) (a) 2. ~~or a student or prospective student~~
25 who is expelled, suspended, disciplined, or otherwise penalized in violation of sub.

an applicant for employment who is not
hired in violation of s.b. (2)(a)3.,

ASSEMBLY BILL 218

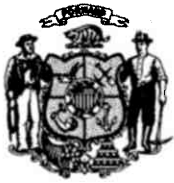
1 (3) (a) 2. ^{, or a prospective student who is not admitted in violation of}
2 the complaint in the same manner as employment discrimination complaints are
3 processed under s. 111.39. If the department finds that a violation of sub. (2) (a) 2.
4 or (3) (a) 2. ^{or 3.} has been committed, the department may order the employer or
5 educational institution to take such action authorized under s. 111.39 as will remedy
6 the violation. Section 111.322 (2m) applies to a discharge or other discriminatory act
7 arising in connection with any proceeding under this paragraph.

8 (c) A tenant or prospective tenant who is discriminated against in violation of
9 sub. (4) (a) 2. may file a complaint with the department, and the department shall
10 process the complaint in the same manner as housing discrimination complaints are
11 processed under s. 106.50. If the department finds that a violation of sub. (4) (a) 2.
12 has been committed, the department may order the landlord to take such action
13 authorized under s. 106.50 as will remedy the violation.

SECTION 6. Initial applicability.

15 (1) COLLECTIVE BARGAINING AGREEMENT. This act first applies to an employee
16 who is affected by a collective bargaining agreement that contains provisions
17 inconsistent with this act on the day on which the collective bargaining agreement
18 expires or is extended, modified, or renewed, whichever occurs first.

19 (END)



State of Wisconsin
2013 - 2014 LEGISLATURE



LRBs0093/7
GMM

1
jld

IN 7117
Wanted 7119

ASSEMBLY SUBSTITUTE AMENDMENT,
TO ASSEMBLY BILL 218

X

Gen

1 AN ACT ...; **relating to:** employer access to, and observation of, the personal
2 Internet accounts of employees and applicants for employment; educational
3 institution access to, and observation of, the personal Internet accounts of
4 students and prospective students; landlord access to, and observation of, the
5 personal Internet accounts of tenants and prospective tenants; and providing
6 a penalty. ✓

Analysis by the Legislative Reference Bureau

Current law does not regulate employer access to, or observation of, the personal Internet accounts of employees and applicants for employment; ^{on} educational institution access to, or observation of, the personal Internet accounts of students and prospective students; or landlord access to, or observation of, the personal Internet accounts of tenants and prospective tenants. ✓ *

This substitute amendment prohibits an employer, educational institution, or landlord from:

1. Requesting or requiring an ✓ employee, applicant for employment, student, prospective student, tenant, or prospective tenant to disclose a user name and password or any other security information (access information) ✓ that protects access

to an Internet-based account that is created and used exclusively for purposes of personal communications (personal Internet account) of the employee, applicant, student, prospective student, tenant, or prospective tenant or to otherwise grant access to or allow observation of that account.

2. Discharging, expelling, suspending, disciplining, or otherwise penalizing or discriminating against an employee, student, tenant, or prospective tenant for exercising the right under the substitute amendment to refuse to disclose that access information or to otherwise grant that access or allow that observation, opposing such a practice, filing a complaint or attempting to enforce that right, or testifying or assisting in any action or proceeding to enforce that right.

3. Refusing to hire an applicant for employment or to admit a prospective student because the applicant or prospective student refused to disclose that access information or to otherwise grant that access or allow that observation.

The substitute amendment, however, permits an employer, educational institution, or landlord to view, access, or use information about an employee, applicant for employment, student, prospective student, tenant, or prospective tenant that can be obtained without access information or that is available from the public domain.

The substitute amendment also permits an employer or educational institution to request or require an employee or student to disclose access information to the employer or educational institution in order for the employer or educational institution to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the employer or educational institution or in order for the employer or educational institution to gain access to an account or service provided by the employer or educational institution, obtained by virtue of the employment relationship or admission to the educational institution, or used for business or educational purposes.

The substitute amendment, in addition, permits an employer to do any of the following:

1. Discharge or discipline an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.

2. Conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account or of any other alleged employment-related misconduct or violation of the law, provided that in conducting or requiring cooperation in such an investigation the employer ~~requires~~ the employee to grant access or ~~or~~ allow observation of the employee's personal Internet account, but ~~does not~~ require the employee to disclose access information for that account.

3. Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device supplied or paid for in whole or in part by the employer (employer-provided electronic communications device) or while using the employer's network or other resources.

* 4. Comply with a duty to screen applicants for employment prior to hiring or a duty to monitor or retain employee communications that is established under state or federal law, rules, or regulations or the rules of a self-regulatory organization, as defined under the federal Securities and Exchange Act of 1934 (self-regulatory organization).✓

5. Requesting or requiring an employee to disclose the employee's personal electronic mail address.✓

In addition, with respect to an employer, the substitute amendment provides: 1) that the prohibition created under the substitute amendment does not apply to a personal Internet account or an electronic communications device of an employee engaged in providing financial services who uses the account or device to conduct the business of an employer that is subject to the content, supervision, and retention requirements imposed by federal securities laws and regulations or by the rules of a self-regulatory organization;✓ and 2) that an employer that inadvertently obtains access information for an employee's personal Internet account through the use of an electronic device or program that monitors the employer's network or through an employer-provided electronic communications device✓ is not liable under the substitute amendment for possessing that access information so long as the employer does not use that access information to access the employee's personal Internet account.✓

Finally, the substitute amendment provides that an employer, educational institution, or landlord does not have a duty to search or monitor the activity of any personal Internet account✓ and is not liable for any failure to request or require access to or observation of a personal Internet account of an employee, applicant for employment, student, prospective student, tenant, or prospective tenant.✓

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

✕

1 **SECTION 1.** 106.54 (10) of the statutes is created to read:

2 106.54 (10) (a) The division✓ shall receive complaints under s. 995.55 (6) (b)✓ and
3 shall process the complaints in the same manner as employment discrimination
4 complaints are processed under s. 111.39.✓

5 (b) The division shall receive complaints under s. 995.55 (6) (c)✓ and shall
6 process the complaints in the same manner as housing discrimination complaints
7 are processed under s. 106.50.✓

8 **SECTION 2.** 111.322 (2m) (a) of the statutes is amended to read:

111.322 (2m) (a) The individual files a complaint or attempts to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, 995.55~~ or ss. 101.58 to 101.599 or 103.64 to 103.82.

SECTION 3. 111.322 (2m) (b) of the statutes is amended to read:

111.322 (2m) (b) The individual testifies or assists in any action or proceeding held under or to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, 995.55~~ or ss. 101.58 to 101.599 or 103.64 to 103.82.

SECTION 4. 111.91 (2) (im) of the statutes is created to read:

111.91 (2) (im) Employer access to the social networking Internet site of an employee that provides fewer rights and remedies to employees than are provided under s. 995.55.

SECTION 5. 995.55 of the statutes is created to read:

995.55 Internet privacy protection. (1) DEFINITIONS. In this section:

(a) "Access information" means a user name and password or any other security information that protects access to a personal Internet account.

(b) "Educational institution" means an institution of higher education, as defined in s. 108.02 (18); a technical college established under s. 38.02; a school, as defined in s. 38.50 (11) (a) 2.; a public school, as described in s. 115.01 (1); a charter school, as defined in s. 115.001 (1); a private school, as defined in s. 115.001 (3r); or a private educational testing service or administrator.

(c) "Employer" means any person engaging in any activity, enterprise, or business employing at least one individual. "Employer" includes the state, its political subdivisions, and any office, department, independent agency, authority,

1 institution, association, society, or other body in state or local government created or
2 authorized to be created by the constitution or any law, including the legislature and
3 the courts.✓

4 (d) “Personal Internet account”✓ means an Internet-based account that is
5 created and used by an individual exclusively for purposes of personal
6 communications.✓

7 (2) RESTRICTIONS ON EMPLOYER ACCESS TO PERSONAL INTERNET ACCOUNTS.✓ (a)
8 Except as provided in pars. (b), (c), and (d),✓ no employer may do any of the following:✓

9 1. Request or require an employee or applicant for employment to disclose
10 access information✓ for the✓ personal Internet account of the employee or applicant or
11 to otherwise grant access to or allow observation of that account.✓

12 2. Discharge or otherwise discriminate against an employee for exercising the
13 right under subd. 1.✓ to refuse to disclose access information for, grant access to, or
14 allow observation of the employee’s personal Internet account, opposing a practice
15 prohibited under subd. 1.✓, filing a complaint or attempting to enforce any right under
16 subd. 1.,✓ or testifying or assisting in any action or proceeding to enforce any right
17 under subd. 1.✓

18 3. Refuse to hire an applicant for employment because the applicant refused
19 to disclose access information for, grant access to, or allow observation of the
20 applicant’s personal Internet account.✓

21 (b) Paragraph (a)✓ does not prohibit an employer from doing any of the following:

22 1. Requesting or requiring an employee to disclose access information to the
23 employer in order for the employer to gain access to or operate an electronic
24 communications device supplied or paid for in whole or in part by the employer or in
25 order for the employer to gain access to an account or service provided by the

1 employer, obtained by virtue of the employee's employment relationship with the
2 employer, or used for the employer's business purposes.✓

3 2. Discharging or disciplining an employee for transferring the employer's
4 proprietary or confidential information or financial data to the employee's personal
5 Internet account without the employer's authorization.✓

6 3. Subject to this subdivision,✓ conducting an investigation or requiring an
7 employee to cooperate in an investigation of any alleged unauthorized transfer of the
8 employer's proprietary or confidential information or financial data to the
9 employee's personal Internet account,✓ if the employer has reasonable cause to
10 believe that such a transfer has occurred, or of any other alleged
11 employment-related misconduct or violation of the law, if the employer has
12 reasonable cause to believe that activity on the employee's personal Internet account
13 relating to that misconduct or violation of the law has occurred. In conducting an
14 investigation or requiring an employee to cooperate in an investigation under this
15 subdivision,✓ an employer may require an employee to grant access to or allow
16 observation of the employee's personal Internet account, but may not require the
17 employee to disclose access information for that account.✓

18 4. Restricting or prohibiting an employee's access to certain✓ Internet sites while
19 using an electronic communications device supplied or paid for in whole or in part
20 by the employer or while using the employer's network or other resources.✓

21 5. Complying with a duty to screen applicants for employment prior to hiring
22 or a duty to monitor or retain employee communications that is established under
23 state or federal laws, rules, or regulations or the rules of a self-regulatory
24 organization, as defined in 15 USC 78c (a) (26).

1 6. Viewing, accessing, or using information about an employee or applicant for
2 employment that can be obtained without access information or that is available in
3 the public domain.✓

4 7. Requesting or requiring an employee to disclose the employee's personal
5 electronic mail address.✓

6 (c) Paragraph (a)✓ does not apply to a personal Internet account or an electronic
7 communications device of an employee engaged in providing financial services who
8 uses the account or device to conduct the business of an employer that is subject to
9 the content, supervision, and retention requirements imposed by federal securities
10 laws and regulations or by the rules of a✓ self-regulatory organization, as defined in
11 15 USC 78c (a) (26).

12 (d) An employer that inadvertently obtains access information for an
13 employee's personal Internet account through the use of an electronic device or
14 program that monitors the employer's network or through an electronic
15 communications device supplied or paid for in whole or in part by the employer is not
16 liable under par. (a)✓ for possessing that access information so long as the employer
17 does not use that access information to access the employee's personal Internet
18 account.✓

19 **(3) RESTRICTIONS ON EDUCATIONAL INSTITUTION ACCESS TO PERSONAL✓ INTERNET**
20 **ACCOUNTS.** (a) Except as provided in par. (b),✓ no educational institution may do any
21 of the following:

22 1. Request or require a student or prospective student✓ to disclose access
23 information for the personal Internet account of the student or prospective student
24 or to otherwise grant access to or allow observation of that account.✓

1 2. Expel, suspend, discipline, or otherwise penalize any student for exercising
2 the right under subd. 1. to refuse to disclose access information for, grant access to,
3 or allow observation of the student's personal Internet account, opposing a practice
4 prohibited under subd. 1., filing a complaint or attempting to enforce any right under
5 subd. 1., or testifying or assisting in any action or proceeding to enforce any right
6 under subd. 1.

7 3. Refuse to admit a prospective student because the prospective student
8 refused to disclose access information for, grant access to, or allow observation of the
9 prospective student's personal Internet account.

10 (b) Paragraph (a) does not prohibit an educational institution from doing any
11 of the following:

12 1. Requesting or requiring a student to disclose access information to the
13 educational institution in order for the institution to gain access to or operate an
14 electronic communications device supplied or paid for in whole or in part by the
15 institution or in order for the educational institution to gain access to an account or
16 service provided by the institution, obtained by virtue of the student's admission to
17 the educational institution, or used for educational purposes.

18 2. Viewing, accessing, or using information about a student or prospective
19 student that can be obtained without access information or that is available in the
20 public domain.

21 (4) RESTRICTIONS ON LANDLORD ACCESS TO PERSONAL INTERNET ACCOUNTS. (a)
22 Except as provided in par. (b), no landlord may do any of the following:

23 1. Request or require a tenant or prospective tenant to disclose access
24 information for the personal Internet account of the tenant or prospective tenant or
25 to otherwise grant access to or allow observation of that account.

1 2. Discriminate in a manner described in s. 106.50 (2) against a tenant or
2 prospective tenant for exercising the right under subd. 1. to refuse to disclose access
3 information for, grant access to, or allow observation of the personal Internet account
4 of the tenant or prospective tenant, opposing a practice prohibited under subd. 1.,
5 filing a complaint or attempting to enforce any right under subd. 1., or testifying or
6 assisting in any action or proceeding to enforce any right under subd. 1.

7 (b) Paragraph (a) does not prohibit a landlord from viewing, accessing, or using
8 information about a tenant or prospective tenant that can be obtained without access
9 information or that is available in the public domain.

10 (5) NO DUTY TO MONITOR. (a) Nothing in this section creates a duty for an
11 employer, educational institution, or landlord to search or monitor the activity of any
12 personal Internet account.

13 (b) An employer, educational institution, or landlord is not liable under this
14 section for any failure to request or require that an employee, applicant for
15 employment, student, prospective student, tenant, or prospective tenant grant
16 access to, allow observation of, or disclose information that allows access to or
17 observation of a personal Internet account of the employee, applicant for
18 employment, student, prospective student, tenant, or prospective tenant.

19 (6) ENFORCEMENT. (a) Any person who violates sub. (2) (a), (3) (a), or (4) (a) may
20 be required to forfeit not more than \$1,000.

21 (b) An employee who is discharged or otherwise discriminated against in
22 violation of sub. (2) (a) 2., an applicant for employment who is not hired in violation
23 of sub. (2) (a) 3., a student who is expelled, suspended, disciplined, or otherwise
24 penalized in violation of sub. (3) (a) 2., or a prospective student who is not admitted
25 in violation of sub. (3) (a) 3., may file a complaint with the department, and the

1 department shall process the complaint in the same manner as employment
2 discrimination complaints are processed under s. 111.39. ✓ If the department finds
3 that a violation of sub. (2) (a) 2. ✓ or 3. ✓ or (3) (a) 2. ✓ or 3. ✓ has been committed, the
4 department may order the employer or educational institution to take such action
5 authorized under s. 111.39 as will remedy the violation. Section ✓ 111.322 (2m) applies
6 to a discharge or other discriminatory act arising in connection with any proceeding
7 under this paragraph. ✓

8 (c) A tenant or prospective tenant who is discriminated against in violation of
9 sub. (4) (a) 2. ✓ may file a complaint with the department, and the department shall
10 process the complaint in the same manner as housing discrimination complaints are
11 processed under s. 106.50. ✓ If the department finds that a violation of sub. ✓ (4) (a) 2.
12 has been committed, the department may order the landlord to take such action
13 authorized under s. 106.50 as will remedy the violation. ✓

14 **SECTION 6. Initial applicability.**

15 (1) COLLECTIVE BARGAINING AGREEMENT. ✓ This act first applies to an employee
16 who is affected by a collective bargaining agreement that contains provisions
17 inconsistent with this act on the day on which the collective bargaining agreement
18 expires or is extended, modified, or renewed, whichever occurs first. ✓

19 (END)

817

Aaron Collins

Also permit employer access to employee social media
violation
to conduct investigation & employer's work rules
specified in an employee handbook



State of Wisconsin
2013 - 2014 LEGISLATURE

6/8/17
5:00 PM



LRBs0093/1
GMM:jld:6
stays
DNR

ASSEMBLY SUBSTITUTE AMENDMENT ,
TO ASSEMBLY BILL 218

gen cat

1 AN ACT *to amend* 111.322 (2m) (a) and 111.322 (2m) (b); and *to create* 106.54
2 (10), 111.91 (2) (im) and 995.55 of the statutes; **relating to:** employer access to,
3 and observation of, the personal Internet accounts of employees and applicants
4 for employment; educational institution access to, and observation of, the
5 personal Internet accounts of students and prospective students; landlord
6 access to, and observation of, the personal Internet accounts of tenants and
7 prospective tenants; and providing a penalty.

Analysis by the Legislative Reference Bureau

Current law does not regulate employer access to, or observation of, the personal Internet accounts of employees and applicants for employment; educational institution access to, or observation of, the personal Internet accounts of students and prospective students; or landlord access to, or observation of, the personal Internet accounts of tenants and prospective tenants.

This substitute amendment prohibits an employer, educational institution, or landlord from:

1. Requesting or requiring an employee, applicant for employment, student, prospective student, tenant, or prospective tenant to disclose a user name and

password or any other security information (access information) that protects access to an Internet-based account that is created and used exclusively for purposes of personal communications (personal Internet account) of the employee, applicant, student, prospective student, tenant, or prospective tenant or to otherwise grant access to or allow observation of that account.

2. Discharging, expelling, suspending, disciplining, or otherwise penalizing or discriminating against an employee, student, tenant, or prospective tenant for exercising the right under the substitute amendment to refuse to disclose that access information or to otherwise grant that access or allow that observation, opposing such a practice, filing a complaint or attempting to enforce that right, or testifying or assisting in any action or proceeding to enforce that right.

3. Refusing to hire an applicant for employment or to admit a prospective student because the applicant or prospective student refused to disclose that access information or to otherwise grant that access or allow that observation.

The substitute amendment, however, permits an employer, educational institution, or landlord to view, access, or use information about an employee, applicant for employment, student, prospective student, tenant, or prospective tenant that can be obtained without access information or that is available from the public domain.

The substitute amendment also permits an employer or educational institution to request or require an employee or student to disclose access information to the employer or educational institution in order for the employer or educational institution to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the employer or educational institution or in order for the employer or educational institution to gain access to an account or service provided by the employer or educational institution, obtained by virtue of the employment relationship or admission to the educational institution, or used for business or educational purposes.

The substitute amendment, in addition, permits an employer to do any of the following:

1. Discharge or discipline an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.

2. Conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account or of any other alleged employment-related misconduct or violation of the law, provided that in conducting or requiring cooperation in such an investigation the employer may require the employee to grant access or allow observation of the employee's personal Internet account, but may not require the employee to disclose access information for that account.

3. Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device supplied or paid for in whole or in part by the employer (employer-provided electronic communications device) or while using the employer's network or other resources.

violation or violation of the employer's work rules as specified in an employee handbook,

4. Comply with a duty to screen applicants for employment prior to hiring or a duty to monitor or retain employee communications that is established under state or federal law, rules, or regulations or the rules of a self-regulatory organization, as defined under the federal Securities Exchange Act of 1934 (self-regulatory organization).

5. Requesting or requiring an employee to disclose the employee's personal electronic mail address.

In addition, with respect to an employer, the substitute amendment provides: 1) that the prohibition created under the substitute amendment does not apply to a personal Internet account or an electronic communications device of an employee engaged in providing financial services who uses the account or device to conduct the business of an employer that is subject to the content, supervision, and retention requirements imposed by federal securities laws and regulations or by the rules of a self-regulatory organization; and 2) that an employer that inadvertently obtains access information for an employee's personal Internet account through the use of an electronic device or program that monitors the employer's network or through an employer-provided electronic communications device is not liable under the substitute amendment for possessing that access information so long as the employer does not use that access information to access the employee's personal Internet account.

Finally, the substitute amendment provides that an employer, educational institution, or landlord does not have a duty to search or monitor the activity of any personal Internet account and is not liable for any failure to request or require access to or observation of a personal Internet account of an employee, applicant for employment, student, prospective student, tenant, or prospective tenant.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

×

1 **SECTION 1.** 106.54 (10) of the statutes is created to read:

2 106.54 (10) (a) The division shall receive complaints under s. 995.55 (6) (b) and
3 shall process the complaints in the same manner as employment discrimination
4 complaints are processed under s. 111.39.

5 (b) The division shall receive complaints under s. 995.55 (6) (c) and shall
6 process the complaints in the same manner as housing discrimination complaints
7 are processed under s. 106.50.

×

8 **SECTION 2.** 111.322 (2m) (a) of the statutes is amended to read:

111.322 (2m) (a) The individual files a complaint or attempts to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, or 995.55~~, or ss. 101.58 to 101.599 or 103.64 to 103.82.

SECTION 3. 111.322 (2m) (b) of the statutes is amended to read:

111.322 (2m) (b) The individual testifies or assists in any action or proceeding held under or to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997~~, or 995.55, or ss. 101.58 to 101.599 or 103.64 to 103.82.

SECTION 4. 111.91 (2) (im) of the statutes is created to read:

111.91 (2) (im) Employer access to the social networking Internet site of an employee that provides fewer rights and remedies to employees than are provided under s. 995.55.

SECTION 5. 995.55 of the statutes is created to read:

995.55 Internet privacy protection. (1) **DEFINITIONS.** In this section:

(a) “Access information” means a user name and password or any other security information that protects access to a personal Internet account.

(b) “Educational institution” means an institution of higher education, as defined in s. 108.02 (18); a technical college established under s. 38.02; a school, as defined in s. 38.50 (11) (a) 2.; a public school, as described in s. 115.01 (1); a charter school, as defined in s. 115.001 (1); a private school, as defined in s. 115.001 (3r); or a private educational testing service or administrator.

(c) “Employer” means any person engaging in any activity, enterprise, or business employing at least one individual. “Employer” includes the state, its political subdivisions, and any office, department, independent agency, authority,

1 institution, association, society, or other body in state or local government created or
2 authorized to be created by the constitution or any law, including the legislature and
3 the courts.

4 (d) “Personal Internet account” means an Internet-based account that is
5 created and used by an individual exclusively for purposes of personal
6 communications.

7 **(2) RESTRICTIONS ON EMPLOYER ACCESS TO PERSONAL INTERNET ACCOUNTS.** (a)
8 Except as provided in pars. (b), (c), and (d), no employer may do any of the following:

9 1. Request or require an employee or applicant for employment to disclose
10 access information for the personal Internet account of the employee or applicant or
11 to otherwise grant access to or allow observation of that account.

12 2. Discharge or otherwise discriminate against an employee for exercising the
13 right under subd. 1. to refuse to disclose access information for, grant access to, or
14 allow observation of the employee’s personal Internet account, opposing a practice
15 prohibited under subd. 1., filing a complaint or attempting to enforce any right under
16 subd. 1., or testifying or assisting in any action or proceeding to enforce any right
17 under subd. 1.

18 3. Refuse to hire an applicant for employment because the applicant refused
19 to disclose access information for, grant access to, or allow observation of the
20 applicant’s personal Internet account.

21 (b) Paragraph (a) does not prohibit an employer from doing any of the following:

22 1. Requesting or requiring an employee to disclose access information to the
23 employer in order for the employer to gain access to or operate an electronic
24 communications device supplied or paid for in whole or in part by the employer or in
25 order for the employer to gain access to an account or service provided by the

1 employer, obtained by virtue of the employee's employment relationship with the
2 employer, or used for the employer's business purposes.

3 2. Discharging or disciplining an employee for transferring the employer's
4 proprietary or confidential information or financial data to the employee's personal
5 Internet account without the employer's authorization.

6 3. Subject to this subdivision, conducting an investigation or requiring an
7 employee to cooperate in an investigation of any alleged unauthorized transfer of the
8 employer's proprietary or confidential information or financial data to the
9 employee's personal Internet account, if the employer has reasonable cause to
10 believe that such a transfer has occurred, or of any other alleged
11 employment-related misconduct ^{or violation of the employer's} ~~or~~ violation of the law, if the employer has

12 reasonable cause to believe that activity on the employee's personal Internet account
13 relating to that misconduct or violation ^{work rules as specified in} ~~of the law~~ an employee handbook, has occurred. In conducting an
14 investigation or requiring an employee to cooperate in an investigation under this
15 subdivision, an employer may require an employee to grant access to or allow
16 observation of the employee's personal Internet account, but may not require the
17 employee to disclose access information for that account.

18 4. Restricting or prohibiting an employee's access to certain Internet sites while
19 using an electronic communications device supplied or paid for in whole or in part
20 by the employer or while using the employer's network or other resources.

21 5. Complying with a duty to screen applicants for employment prior to hiring
22 or a duty to monitor or retain employee communications that is established under
23 state or federal laws, rules, or regulations or the rules of a self-regulatory
24 organization, as defined in 15 USC 78c (a) (26).

1 6. Viewing, accessing, or using information about an employee or applicant for
2 employment that can be obtained without access information or that is available in
3 the public domain.

4 7. Requesting or requiring an employee to disclose the employee's personal
5 electronic mail address.

6 (c) Paragraph (a) does not apply to a personal Internet account or an electronic
7 communications device of an employee engaged in providing financial services who
8 uses the account or device to conduct the business of an employer that is subject to
9 the content, supervision, and retention requirements imposed by federal securities
10 laws and regulations or by the rules of a self-regulatory organization, as defined in
11 15 USC 78c (a) (26).

12 (d) An employer that inadvertently obtains access information for an
13 employee's personal Internet account through the use of an electronic device or
14 program that monitors the employer's network or through an electronic
15 communications device supplied or paid for in whole or in part by the employer is not
16 liable under par. (a) for possessing that access information so long as the employer
17 does not use that access information to access the employee's personal Internet
18 account.

19 **(3) RESTRICTIONS ON EDUCATIONAL INSTITUTION ACCESS TO PERSONAL INTERNET**
20 **ACCOUNTS.** (a) Except as provided in par. (b), no educational institution may do any
21 of the following:

22 1. Request or require a student or prospective student to disclose access
23 information for the personal Internet account of the student or prospective student
24 or to otherwise grant access to or allow observation of that account.

2. Expel, suspend, discipline, or otherwise penalize any student for exercising the right under subd. 1. to refuse to disclose access information for, grant access to, or allow observation of the student's personal Internet account, opposing a practice prohibited under subd. 1., filing a complaint or attempting to enforce any right under subd. 1., or testifying or assisting in any action or proceeding to enforce any right under subd. 1.

3. Refuse to admit a prospective student because the prospective student refused to disclose access information for, grant access to, or allow observation of the prospective student's personal Internet account.

(b) Paragraph (a) does not prohibit an educational institution from doing any of the following:

1. Requesting or requiring a student to disclose access information to the educational institution in order for the institution to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the institution or in order for the educational institution to gain access to an account or service provided by the institution, obtained by virtue of the student's admission to the educational institution, or used for educational purposes.

2. Viewing, accessing, or using information about a student or prospective student that can be obtained without access information or that is available in the public domain.

(4) RESTRICTIONS ON LANDLORD ACCESS TO PERSONAL INTERNET ACCOUNTS. (a) Except as provided in par. (b), no landlord may do any of the following:

1. Request or require a tenant or prospective tenant to disclose access information for the personal Internet account of the tenant or prospective tenant or to otherwise grant access to or allow observation of that account.

1 2. Discriminate in a manner described in s. 106.50 (2) against a tenant or
2 prospective tenant for exercising the right under subd. 1. to refuse to disclose access
3 information for, grant access to, or allow observation of the personal Internet account
4 of the tenant or prospective tenant, opposing a practice prohibited under subd. 1.,
5 filing a complaint or attempting to enforce any right under subd. 1., or testifying or
6 assisting in any action or proceeding to enforce any right under subd. 1.

7 (b) Paragraph (a) does not prohibit a landlord from viewing, accessing, or using
8 information about a tenant or prospective tenant that can be obtained without access
9 information or that is available in the public domain.

10 (5) NO DUTY TO MONITOR. (a) Nothing in this section creates a duty for an
11 employer, educational institution, or landlord to search or monitor the activity of any
12 personal Internet account.

13 (b) An employer, educational institution, or landlord is not liable under this
14 section for any failure to request or require that an employee, applicant for
15 employment, student, prospective student, tenant, or prospective tenant grant
16 access to, allow observation of, or disclose information that allows access to or
17 observation of a personal Internet account of the employee, applicant for
18 employment, student, prospective student, tenant, or prospective tenant.

19 (6) ENFORCEMENT. (a) Any person who violates sub. (2) (a), (3) (a), or (4) (a) may
20 be required to forfeit not more than \$1,000.

21 (b) An employee who is discharged or otherwise discriminated against in
22 violation of sub. (2) (a) 2., an applicant for employment who is not hired in violation
23 of sub. (2) (a) 3., a student who is expelled, suspended, disciplined, or otherwise
24 penalized in violation of sub. (3) (a) 2., or a prospective student who is not admitted
25 in violation of sub. (3) (a) 3., may file a complaint with the department, and the

1 department shall process the complaint in the same manner as employment
2 discrimination complaints are processed under s. 111.39[✓]. If the department finds
3 that a violation of sub. (2) (a) 2. or 3. or (3) (a) 2. or 3. has been committed, the
4 department may order the employer or educational institution to take such action
5 authorized under s. 111.39 as will remedy the violation. Section 111.322 (2m)[✓] applies
6 to a discharge or other discriminatory act arising in connection with any proceeding
7 under this paragraph.

8 (c) A tenant or prospective tenant who is discriminated against in violation of
9 sub. (4) (a) 2. may file a complaint with the department, and the department shall
10 process the complaint in the same manner as housing discrimination complaints are
11 processed under s. 106.50. If the department finds that a violation of sub. (4) (a) 2.
12 has been committed, the department may order the landlord to take such action
13 authorized under s. 106.50 as will remedy the violation.

14 **SECTION 6. Initial applicability.**

15 (1) COLLECTIVE BARGAINING AGREEMENT. This act first applies to an employee
16 who is affected by a collective bargaining agreement that contains provisions
17 inconsistent with this act on the day on which the collective bargaining agreement
18 expires or is extended, modified, or renewed, whichever occurs first.

19 (END)